THE NEW REALITY OF RISK

A FRAMEWORK FOR MANAGING CYBER RISK

APRIL 2015

MARSH

CYBER RISK IS HERE TO STAY

"Even an unlimited budget for information security will not eliminate your cyber risk."

— Tom Reagan
Marsh Cyber Practice Leader

A FRAMEWORK FOR MANAGING CYBER RISK

SIMPLIFIED CYBER RISK MANAGEMENT FRAMEWORK

A FRAMEWORK FOR MANAGING CYBER RISK

MANAGING CYBER RISK ACROSS THE ENTERPRISE

Making cyber risk a corporate risk management issue means engaging areas across the enterprise, including:

- Finance.
- Legal.
- Compliance.
- Operations.
- HR.
- Board.
- IT.

A FRAMEWORK FOR MANAGING CYBER RISK

REGULATORY SCRUTINY INCREASING

Four steps to managing regulatory scrutiny:

1. Don’t leave cyber risk to just the IT department.
2. Look beyond attack prevention.
3. Connect your plans to external stakeholders and resources.
4. Include risk transfer as part of the approach.

A FRAMEWORK FOR MANAGING CYBER RISK

THREAT LANDSCAPE

	NUISANCE	DATA THEFT	CYBER CRIME	HACKTIVISM	DESTRUCTIVE ATTACK
OBJECTIVE	Access & Propagation	Economic, Political Advantage	Financial Gain	Defamation, Press & Policy	Disrupt Operations
EXAMPLE	Botnets & Spam	Advanced Persistent Threat Group	Credit Card Theft	Website Defacements	Deletion of Data
TARGETED	☒	☑	☑	☑	☑
CHARACTER	Often Automated	Persistent	Frequently Opportunistic	Conspicuous	Conflict Driven

Source: Mandiant

A FRAMEWORK FOR MANAGING CYBER RISK

WHAT'S AHEAD

2015 and beyond…

- More destructive attacks?
- Attribution will be more important.
- Counter-forensics will improve.
- Attacks will align with conflicts.
- More threat actors will emerge.
- More government involvement.
- A return to standards for non-regulated industries.
- More reliance on the cloud.
- More active defense (hunting).
- Cyber security will continue to be a board issue.

Source: Mandiant

A FRAMEWORK FOR MANAGING CYBER RISK

SECURITY OPERATIONS CHALLENGES

Tools & Technology

- Lack endpoint detection.
- No live response.
- Data (event) overload.
- Slow searches.
- Rely on signature based detection.
- Needle in a haystack.

+

Incident Response

- No threat intel.
- Lack of intel context.
- No hunting.
- Ability to quickly sweep and contain.
- Leverage analytics and anomaly detection.

+

Governance

- Wide mission.
- Lack required skill sets.
- Compliance burden.
- R&R do not align with organizational model.

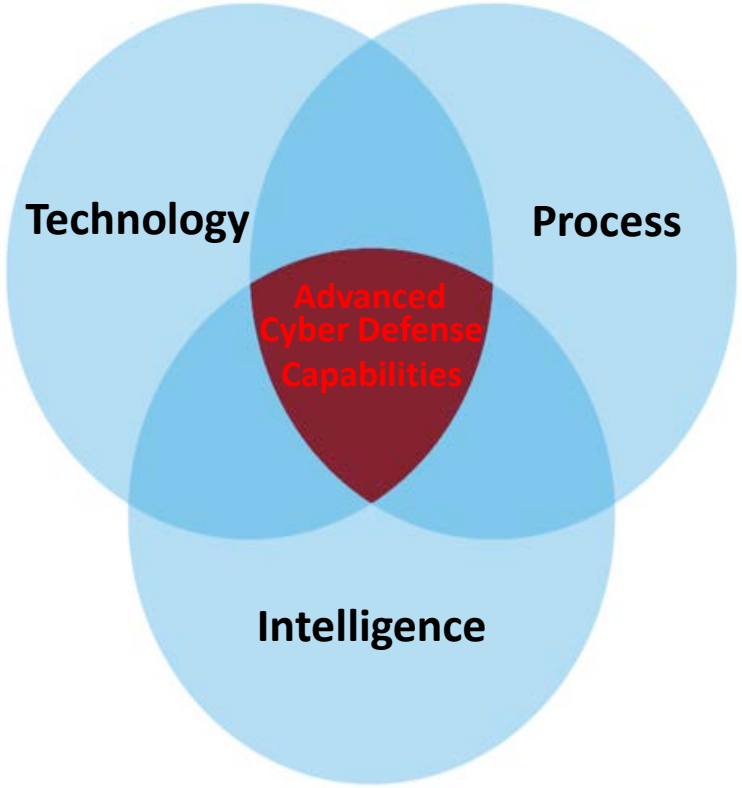
Source: Mandiant

A FRAMEWORK FOR MANAGING CYBER RISK

EFFECTIVE CYBER DEFENSE

Minimize organizational risk and allow business to function while under continuous attack.

- **Predictive** — Continuously measure enterprise attack surface and model potential threat vectors targeted at critical assets and data.
- **Proactive —** Hunt for intrusions. Discover and remediate / compensate for vulnerabilities.
- **Responsive** — Rapid analysis and containment of threats.



Source: Mandiant

A FRAMEWORK FOR MANAGING CYBER RISK

EFFECTIVE CYBER DEFENSE: INDICATORS OF COMPROMISE

- Hunting the network provides the capability to conduct proactive analysis to develop new indicators of compromise (IOC).
  - Mining historical data.
  - IOC sweeps.
- A mature IOC capability includes:
  - Dedicated individuals to design and build IOCs.
  - Develop and update IOCs regularly (IOC editor).
  - Processes and tools in place to actively check systems for IOCs.
- Post-incident, hunting assists in ensuring remediation and eradication activities are successful.

Source: Mandiant

A FRAMEWORK FOR MANAGING CYBER RISK

INTELLIGENCE IS KING

Commodity	• Generated from commodity malware analysis. o Structured output — artifacts, domains, MD5s.
Curated	• Generated from FireEye research and profiling. o Unstructured output; APT groups, TTPs, landscape.
Community	• Generated by sharing with industry partners. o Structured and unstructured outputs, validate intelligence.

Source: Mandiant

A FRAMEWORK FOR MANAGING CYBER RISK

CYBER RISK: A RISK MANAGER'S VIEW

- Cyber risk at John Deere means:
  1. The risk of unauthorized access to personally identifiable information (PII).
  2. The risk from employee health and HR records, intellectual property, and credit card transactions.

- Focus has been on PII:
  - How much we have.
  - Where and how it's stored.
  - What we would do if it was lost.

- Deere is known as a manufacturer, but has a substantial captive finance unit.

Source: Deere & Co.

A FRAMEWORK FOR MANAGING CYBER RISK

CYBER RISK MANAGEMENT EVOLVES

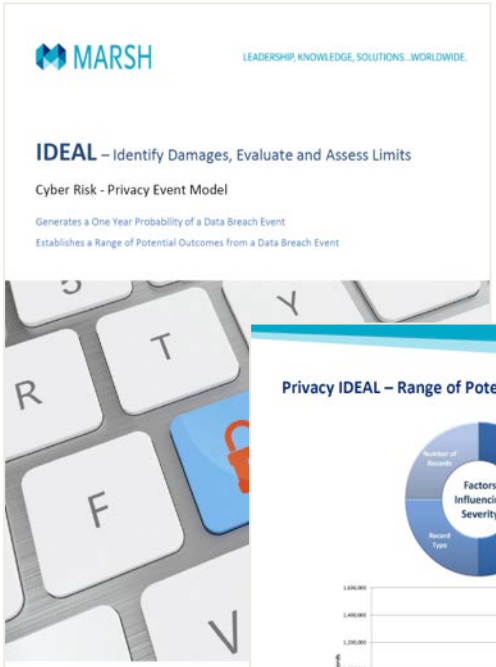
- Cyber insurance:
  - At Deere, cyber tower has evolved from an engineering E&O policy covering a small contract electronics manufacturing operation that we acquired.
  - Each year we gain a greater understanding of cyber exposures.
  - Closer attention to policy terms and limits, increasing limits at several renewals.
  - Able to demonstrate a robust insurance program to C-suite.

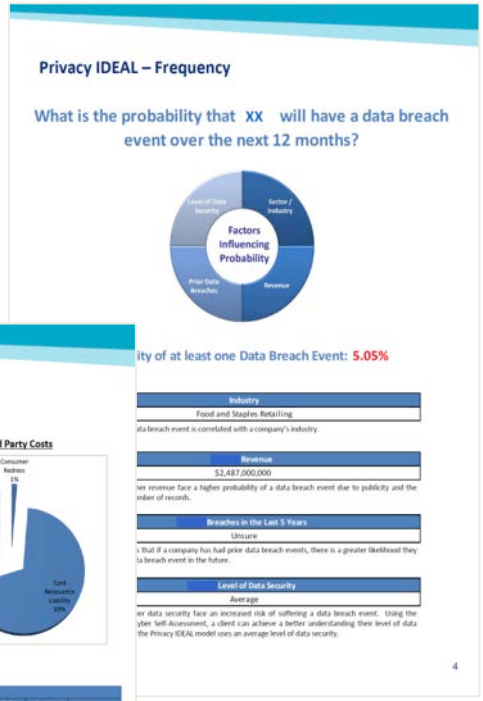
- Risk management:
  - Learned that there are many cyber stakeholders.
  - Effective cyber insurance needs to be aligned with their interests.
  - IT, legal, compliance, and security.
  - Build relationships and partnerships.
  - They, in turn, appreciate our understanding of the risks and the company's exposures.

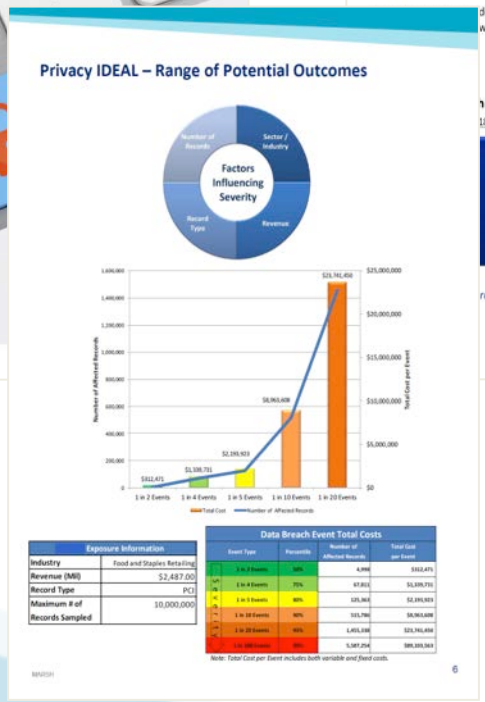
Source: Deere & Co.

A FRAMEWORK FOR MANAGING CYBER RISK

CYBER IDEAL: PRIVACY EVENT MODEL







"When the C-suite asked about cyber, we were able to demonstrate that a robust insurance program was already in place."

— James P. Morley
Manager, Risk Analysis, Deere & Co.

A FRAMEWORK FOR MANAGING CYBER RISK

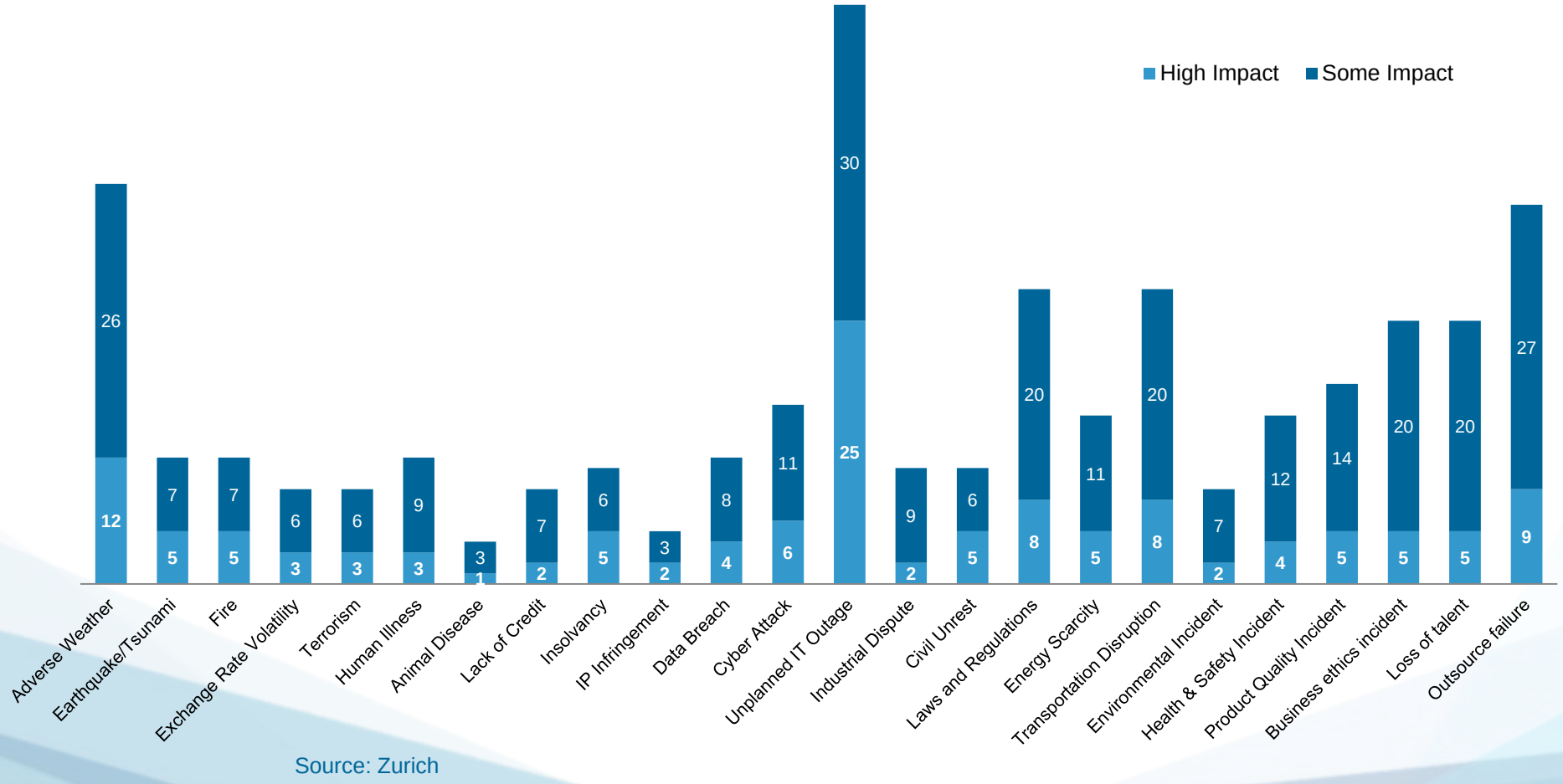
CYBER INSURANCE: CATEGORIES OF RISK

COVERAGE	DESCRIPTION
Information Asset Loss	The cost to restore data compromised or deleted during a network attack.
Cyber Extortion Expenses	Costs to pay an extortionist's demands.
Business interruption and Extra Expense	Reimbursement of lost business income and extra expense following a network failure, including coverage for contingent business interruption.
Privacy and Network Security Liability	• Investigation, assessment, and notification costs in the event of a data breach. • Defense and liability resulting from a claim for a security breach. • Defense and liability resulting from a claim for a privacy breach • Counsel for a privacy regulatory proceeding or investigation • Indemnification of any fines or penalties assessed by the regulator from the privacy breach.

A FRAMEWORK FOR MANAGING CYBER RISK

SUPPLY CHAIN DISRUPTIONS

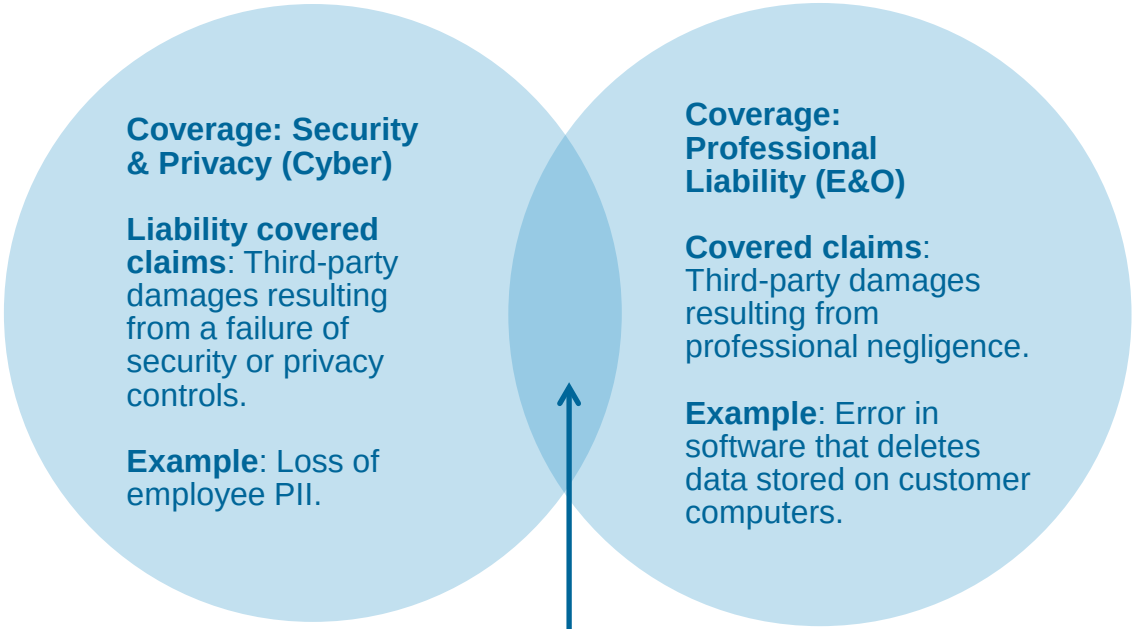
Unplanned network outages: The most significant supply chain disruption exposure.



Source: Zurich

A FRAMEWORK FOR MANAGING CYBER RISK

CYBER AND PROFESSIONAL LIABILITY: HOW DO THEY OVERLAP?



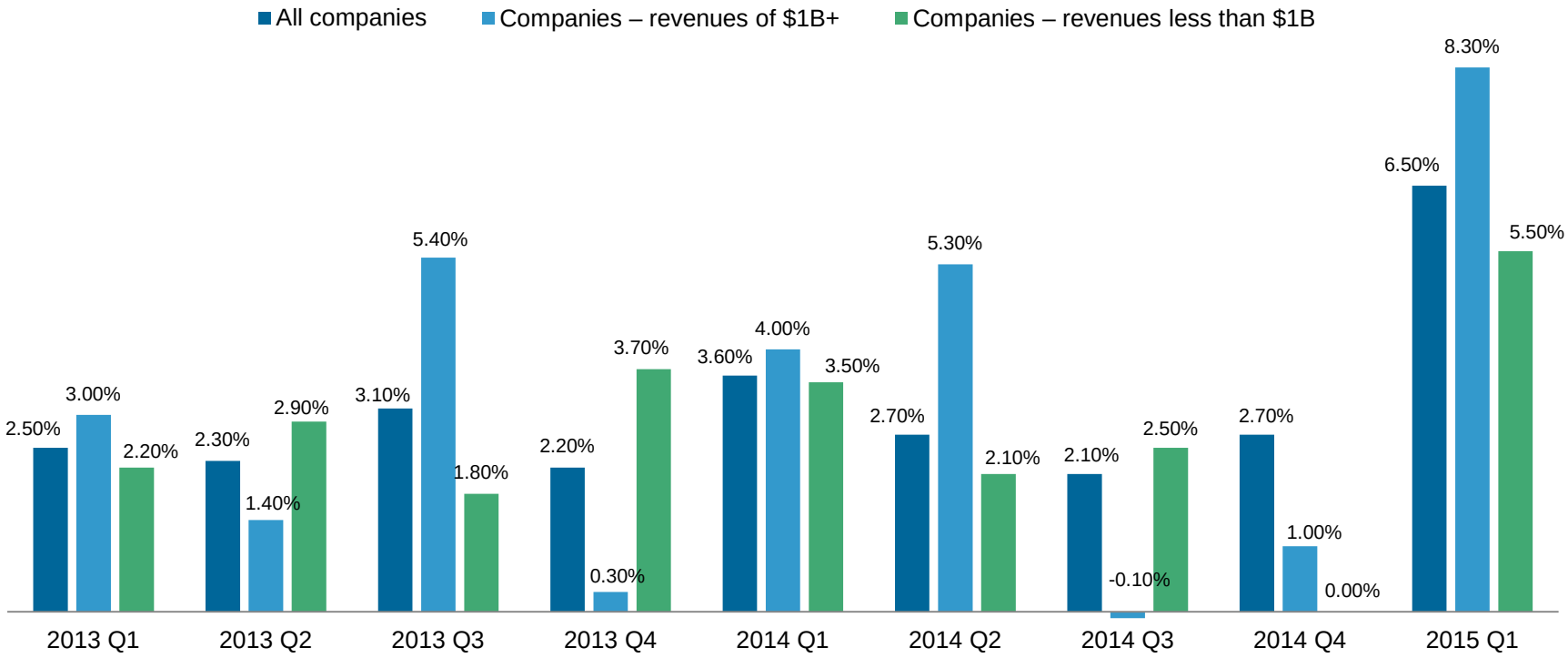
Third-party damages resulting from coincidence of control failure *and* professional negligence.

Example: Security breach that discloses customer information.

A FRAMEWORK FOR MANAGING CYBER RISK

CYBER INSURANCE RATES

US HISTORICAL RATE (TOTAL PRICE PER MILLION) CHANGES – CYBER LIABLIITY



A FRAMEWORK FOR MANAGING CYBER RISK

MARSH

Benchmarking Trends:
As Cyber Concerns Broaden,
Insurance Purchases Rise

Cyber-attacks are escalating in their frequency and intensity, and pose a growing threat to the business community as well as the national security of countries. High-profile cyber incidents in 2014 reflected the expanding spectrum of cyber threats — from point-of-sale (POS) breaches against customer accounts to targeted denial-of-service (DoS) attacks meant to disable a company's network. Insureds in ever-larger numbers sought financial protection through insurance, buying coverage for losses from data breaches and due to business outages. In 2014, the number of US-based Marsh clients purchasing standalone cyber insurance increased 32% over 2013 (see **FIGURE 1**). The cyber take-up rate — the percentage of existing Marsh financial and professional liability clients that purchased cyber insurance — rose to 16%. Early evidence in 2015 shows a continued acceleration in the demand for cyber insurance.

BOOST IN CYBER INSURANCE DEMAND DRIVES INSURERS' RESPONSE

Health care facilities, universities, and schools continue to be on cybercriminals' radar, but attacks in the hospitality and gaming, power and utilities, and other sectors, reveal that no organization is immune to a cyber-attack or failure of technology. Health care and education clients had the highest cyber insurance take-up rates in 2014 at 50% and 32%, respectively, followed by hospitality and gaming (26%) and services (22%). Universities and schools present attractive targets because they house a vast array of personal information of students, parents, employees, alumni, and others: Social Security numbers, health care information, financial data, and research papers can all be compromised.

The broader scope of hacktivists contributed to the increase in cyber insurance purchases in 2014. Sectors that again showed notable year-over-year increases in the number of clients purchasing cyber coverage included hospitality

FIGURE 1 | CYBER INSURANCE TAKE-UP AND GROWTH RATES BY INDUSTRY

Source: Marsh Global Analytics

Cyber Insurance Purchasing

For a copy of ***As Cyber Concerns Broaden, Insurance Purchases Rise***, please visit marsh.com, ask your Marsh representative, or send a request to questions@marsh.com.